مدى وعي أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبراني في ظل التحول الرقمي – دراسة تطبيقية بجامعة الزاوية

نشوه إسماعيل زقوت
كلية الاقتصاد العجيلات- جامعة الزاوية
N.zaqout@zu.edu.ly

سناء أحمد السائح
كلية الاقتصاد العجيلات- جامعة الزاوية
S.asayh@zu.edu.ly

الصديق عبد القادر العطاب
كلية التقنية الهندسية – صرمان
It2017cisco@gmail.com

الملخص:

هدفت الدراسة إلى معرفة درجة وعي أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبراني في ظل التحول الرقمي تحديدا في جامعة الزاوية. ولتحديد أهداف هذه الدراسة تم إتباع المنهج الوصفي التحليلي، وكانت أداة الدراسة عبارة عن استبيان إلكتروني اشتمل على ثلاثة أقسام: القسم الأول تضمن معلومات شملت متغيرات الجنس، المؤهل العلمي، الخبرة العملية، أما القسم الثاني فتضمن ما يتعلق بدرجة الأمن السيبراني (24) فقرة، وتضمن القسم الثالث انتهاكات و مخاطر الأمن السيبراني، وتضمن (6) فقرات، وطُبقت الاستبانة على عينة بلغت (138) عضو هيئة تدريس، وتوصلت الدراسة إلى نتائج أهمها وجود علاقة ذات دلالة إحصائية بين وعي أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبراني في ظل التحول الرقمي في محل الدراسة.

وقدمت الدراسة مجموعة من التوصيات جاء أبرزها طلب عقد دورات تدريبية لأعضاء هيئة التدريس تخص الأمن السيبراني وإدراج مجال الأمن السيبراني ضمن مناهج التعليم في المدارس والجامعات بالإضافة إلى تشجيع بحوث ودراسات الأمن السيبراني في دراسات الماجستير والدكتوراه وإجراء دراسات حول مخاطر الجرائم السيبرانية.

كلمات مفتاحيه: الأمن السيبراني، التحول الرقمي، جامعة الزاوية، استبيان إلكتروني.

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

The extent of awareness of faculty members in Libyan universities about the importance of cyber security in light of digital transformation- Applied study at the University of Zawia

Abstract:
The study aimed to know the degree of awareness of faculty members in Libyan universities about the importance of cybersecurity in light of digital transformation, specifically at Al-Zawia University. Academic qualification, practical experience, while the second section included what is related to the degree of cybersecurity (24 paragraphs), and the third section included cybersecurity violations and risks, and included (6) paragraphs, and the questionnaire was applied to a sample of (138) faculty member, and the study concluded that: The most important results are the existence of a statistically significant relationship between the awareness of faculty members in Libyan universities of the importance of cybersecurity in light of the digital transformation in the study. The study presented a set of recommendations, the most prominent of which was the request to hold training courses for faculty members related to cybersecurity and the inclusion of the field of cybersecurity within the education curricula in schools and universities, in addition to encouraging cybersecurity research and studies in master's and doctoral studies and conducting studies on the risks of cybercrime.
Keywords: cyber security - digital transformation - University of Zawia.

مقدمة:

إن قضية أمن وحماية المعلومات تعتبر من أهم قضايا العصر- عصر الثورة الصناعية الرابعة، حيث أصبح نجاح أي مؤسسة يعتمد بشكل كبير على ما تمتلكه من معلومات، وبالأخص المؤسسات التعليمية فهي ليست بمعزل عن التحول الرقمي الذي يشهده العالم في شتى المجالات. لكن العديد من المعلومات والأنظمة والبنى التحتية المتصلة بالشبكات عرضة للخطر بين الحين والآخر، حيث تواجه أنواعاً شتى من خروقات المعلومات، كما

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

تتعرض لأنشطة إجرامية تعطل خدماتها وتدمر ممتلكاتها؛ وتختلف الهجمات من جهة لأخرى ومن مكان لآخر ومن زمن إلى زمن مستخدمة أدوات وآليات اختراق متجددة ومتطورة طول الوقت.

ومع انفجار الثورة المعلوماتية ودخول العصر الرقمي خاصة في القرن الحادي والعشرين وما نتج عنه من تداعيات عديدة بسبب ظهور تهديدات وجرائم سيبرانية أصبحت تشكل تحدياً كبيراً للأمن القومي وكذلك الدولي، لدرجة أن العديد من الباحثين اعتبر الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء؛ وهو ما استدعى ضرورة وجود ضمانات أمنية ضمن هذه البيئة الرقمية، تبلورت بشكل أساسي في ظهور الأمن كبعد جديد ضمن أجندة حقل الدراسات الأمنية، والتحول الرقمي أو ما يطلق عليه بالرقمنه ما هو إلا عملية تحويل نظام الأعمال لأي قطاع أو مؤسسة إلى نظام يعتمد بشكل رئيسي على التكنولوجيا الرقمية وذلك من اجل تيسير وتسهيل عمل هذه المؤسسات ومنها المؤسسة التعليمية، والتي شهدت بدورها تحول متسارع واعتماد متزايد على التكنولوجيا الرقمية الأمر الذي يساعدها على تطوير و تحسين مخرجاتها العلمية والتعليمية.

والأمن في الفضاء السيبراني يعتبر أمراً مهماً بالنسبة للدول، والمؤسسات، والأفراد (العريشي والدوسري ،2018 : 302) لذا بدأت كثير من الدول والمؤسسات خاصةً التعليمية منها بتبني وتطبيق أمن المعلومات وممارسة الأمن السيبراني وتوفير متطلباته (الجندي ومحمد، 2019: 15 :).

وأشارت كثير من الدراسات إلى أن هناك حراك كبير في العالم أجمع نحو أمن المعلومات والشبكات والأمن السيبراني، من خلال الانضمام لاتفاقيات محاربة جرائم الانترنت. كما تركز المؤسسات التعليمية على تحقيق أعلى استفادة من تكنولوجيا المعلومات والاتصالات مع حماية أنظمتها حفاظاً على سرية بياناتها وحماية الشبكات والأنظمة، حيث تتجه هذه المؤسسات نحو تطويع سياساتها وتوعية وتثقيف العاملين بها بمتطلبات الأمن السيبراني (القحطاني، 2019 ؛ والجندي ومحمد، 2019 ؛ والموجي ومحمود وإمام،. 2021).

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

لقد أصبحت دراسة الأمن السيبراني واحدة من أهم مستحدثات التطور التكنولوجي والرقمي الذي نعايشه في العالم مؤخراً، حيث يشهد العالم المتقدم بكافة أرجائه تطوراً كبيراً لا يمكننا بأي حال أن نغفله. لذا أصبحت تلك الدراسات التكنولوجية مقصد الكثير من الدارسين حول العالم، ومن هذا المنطلق جاءت هذه الدراسة لمحاولة الكشف عن مدى أهمية الأمن السيبراني في ظل التحول الرقمي، ولغرض تحقيق ذلك قد تم تصميم استمارة استبيان تنسجم مع مجتمع البحث لتحديد درجة وعي أعضاء هيئة التدريس بجامعة الزاوية بأهمية الأمن السيبراني في ظل التحول الرقمي.

وقد تضمن البحث عدة محاور رئيسة تمثل الأول منها بالمنهجية البحثية، في حين تناول المحور الثاني الإطار النظري وتضمن المحور الثالث الإطار العملي (تحليل البيانات)، وأخيراً تم استعراض النتائج والمقترحات.

أولا الإطار المنهجي:

1.1المشكلة البحثية:

يعد الأمن السيبراني مكوناً أساسياً من مكونات ومتطلبات أي تحول رقمي؛ حيث إن حماية البيانات والبنية التحتية ستكون مصدر قلق كبير للحكومة والعامة و العديد من القطاعات بما فيها القطاع التعليمي، و بسبب نمو الهجمات السيبرانية أصبح من الضروري التعامل مع مثل هذه الهجمات ومعالجتها بشكل مبتكر ؛ ويعد الأمن السيبراني الحل الأمثل لمتابعة الاستخدام الواسع للإنترنت، وتطبيقاته وأنظمته المختلفة، و للتقليل من المخاطر التي تنشأ من سوء الاستخدام، حيث توجد محتويات غير مشروعة وغير مرغوب بها ذات تأثير سلبي على أخلاقيات وقيم المجتمع، والتي بدورها تؤدي إلى تغييرات في شخصية الأفراد، وتعزز ميلهم للانحراف (الصانع والسواط وأبو عيشة وسليمان وعسران ،2020: 49)

وفي ظل اجتياح الثورة الصناعية الرابعة (الذكاء الاصطناعي وانترنت الأشياء) وارتفاع نسبة المستخدمين من أعضاء هيئة التدريس للإنترنت وما يرتبط بهذا الاستخدام من مفاهيم تتعلق بالأمن السيبراني ولتفادي حدوث الجرائم الالكترونية عليه نطرح التساؤل الرئيسي:

– ما مدى وعي أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبراني في ظل التحول الرقمي؟

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

2.1 أسئلة البحث:

تم صياغة التساؤلات البحثية على النحو الأتي:

- ما هو مفهوم الأمن السيبراني؟
- ما هي أهمية وأهداف الأمن السيبراني في عصر التحول الرقمي؟
- ما هي التهديدات والمخاطر السيبرانية ؟
- ما هي طرق الوقاية من المخاطر والتهديدات؟
- ما درجة وعي أعضاء هيئة التدريس بالجامعات الليبية بمفهوم الأمن السيبراني؟
- ما درجة وعي أعضاء هيئة التدريس بالجامعات الليبية بمخاطر وانتهاكات الأمن السيبراني؟

3.1 أهميه البحث وأسباب اختياره:

- يعد البحث من البحوث القليلة جداً التي تناقش درجة الوعي لأعضاء هيئة التدريس بالجامعات الليبية بالدور المهم الذي يلعبه الأمن السيبراني في ضمان بيئة مناسبة لتبادل المعلومات.
- تساعد هذه الدراسة على توضيح أهمية الأمن السيبراني في عصر التحول الرقمي.
- يُظهر هذا البحث الضرورة الملحة لتعزيز ورفع درجة الوعي بأهمية الأمن السيبراني لدى أعضاء هيئة التدريس بالجامعات الليبية.
- نشر الوعي بالأمن السيبراني لجميع الطلاب والموظفين في الجامعات.

4.1 أهداف البحث:

تتمثل أهدافه فيما يلي:

- السعي للتعرف على درجة وعي أعضاء هيئة التدريس بالجامعات الليبية وتحديداً بجامعة الزاوية بأهمية الأمن السيبراني في ظل التحول الرقمي.
- الكشف عن درجة وعي أعضاء هيئة التدريس بمخاطر وانتهاكات الأمن السيبراني.
- محاولة توضيح طرق الحماية من المخاطر والانتهاكات السيبرانية.

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

5.1 منهجية البحث:

المنهج الوصفي هو المنهج المناسب لإجراء هذه الدراسة وقد كان اختيارنا لهذا المنهج نظرا لطبيعة موضوع الدراسة والذي يتطلب الوصف والتحليل في كلا جانبي الدراسة النظري والتطبيقي.

6.1 حدود الدراسة:

- حدود مكانية :تقتصر هذه الدراسة على جامعة الزاوية.
- حدود بشرية: تقتصر هذه الدراسة على أعضاء هيئة التدريس بالجامعة .
- حدود زمانية :تم إجراء هذه الدراسة في العام الدراسي :2021 -2022

7.1 الدراسات السابقة:

- أجرى كل من يولفين ووانجين (Ulven, & Wangen, 2021) دراسة بهدف مراجعة الأدبيات ذات العلاقة بمخاطر الأمن السيبراني في مؤسسات التعليم العالي، واستخدمت الدراسة الأسلوب المكتبي، حيث تبين أن الأبحاث التجريبية في مجال مخاطر الأمن السيبراني نادرة، وتبين وجود فجوة كبيرة في نتائج الدراسات والبحوث التي تمت مراجعتها على فترة زمنية تجاوزت 12 عام، لكن تبين وجود اتفاق كبير حول متطلبات ومصادر الأمن السيبراني ، وأهمية الأمن السيبراني في حماية وأمن المعلومات، كما تبين أن هناك تسع مخاطر إلكترونية حقيقية بحاجة إلى أمن سيبراني.
- هدفت دراسة (القحطاني 2019) إلى التعرف على مدى توافر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية: (جامعة الأمير نايف، وجامعة الأميرة نورة، وجامعة الإمام محمد بن سعود، وجامعة الجوف، وجامعة الملك خالد، وجامعة الملك سعود، وجامعة الملك عبدالعزيز ، وجامعة الملك فيصل، وجامعة شقراء)، وتم استخدام منهج المسح الاجتماعي بالعينة، واعتمدت الدراسة على الاستبانة في جمع البيانات، حيث أجريت على(486) طالباً وطالبة، وجاءت أهم النتائج أن أقرب مفهوم للأمن السيبراني من وجهة نظر العينة هو استخدام مجموعة الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به، ومنع سوء الاستغلال واستعادة المعاملات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها، وجاءت أبرز الجرائم

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

الإلكترونية التي يعيها الطلبة الاحتيال الإلكتروني، كما تبين وجود معوقات اجتماعية في تحقيق الوقاية من مشكلات الفضاء السيبراني.

- وهدفت دراسة كل من (الجندي ومحمد 2019) إلى التحقق من دور الممارسة التطبيقية للأمن السيبراني في تنمية المهارات ودقة التطبيق العملي للأمن المعلوماتي لدى طالبات الجامعة، وتم الاعتماد على المنهج التكنولوجي التطويري المنظومي، وتم توظيف المنهج الوصفي وشبه التجريبي، وطبقت الدراسة على (80) طالبة من طالبات قسم الحاسب الآلي بالكلية الجامعية جامعة أم– القرى، وتم تقسيمهن إلى مجموعتين الأولى ضابطة والثانية تجريبية، وأشارت النتائج إلى تفوق طالبات المجموعة التجريبية على طالبات المجموعة الضابطة في المهارات ودقة التطبيق العملي للأمن المعلوماتي ، مما يشير إلى وجود دور مهم للممارسة التطبيقية للأمن السيبراني في تنمية المهارات ودقة التطبيق العملي للأمن المعلوماتي لدى طالبات الجامعة.

ثانيا الإطار النظري:

2–1 مفهوم الأمن السيبراني:الأمن السيبراني من حيث المفهوم أوسع وأكثر شمولاً من أمن المعلومات، حيث يتضمن تأمين البيانات والمعلومات التي تُتداول عبر المؤسسات الداخلية والخارجية، والتي يتم تخزينها في خوادم داخل وخارج الهيئات من الاختراق (الموجي ومحمود وإمام، 2021 م، ص21)

وعُرف الأمن السيبراني بأنه حماية الأفراد وبياناتهم وحساباتهم من الهجمات الإلكترونية (الصانع والسواط وأبو عيشة وسليمان وعسران، 2020 : 48)

كما عُرف الأمن السيبراني على أنه عمليات الحماية التي تقوم بها الدولة أو المؤسسات أو الأفراد؛ لحماية العمليات المرتبطة بتقنيات الاتصالات والمعلومات للحد من الخسائر والأضرار والجرائم المرتبطة بهذه التقنيات (القحطاني، 2019 : 91).

فالأمن السيبراني طريقة مثلى لحماية الأنظمة والشبكات والبرامج من الهجمات الرقمية، وذلك بهدف الولوج للمعلومات المهمة ومحاولة إتلافها أو الابتزاز من خلالها للمستخدمين (الغامدي، 2018 : 7).

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

عُرف أيضا الأمن السيبراني بأنه مجموعة من المهمات تتمثل في تجميع الوسائل والسياسات والإجراءات الأمنية والمبادئ التوجيهية والمقاربات لإدارة المخاطر والتدريبات وممارسات آمنة، وتقنيات يمكن استخدامها لحماية البيئة السبرانية وموجودات المؤسسات والمستخدمين (الاتحاد الدولي للاتصالات 2011 : 17)

ومن خلال ما سبق يمكن تعريف الأمن السيبراني انه يمثل مفهوم أمني خاص بحماية المعلومات و كل ما له صلة بتلك المعلومات من عمليات وأجهزة و تقنيات ضد أي شكل من أشكال الوصول الغير مسموح به ، أو استخدام تلك المعلومات بشكل سلبي.

2-2 أهداف الأمن السيبراني:

أشار كل من (السمحان، 2020 :12 ؛ المنتشري، 2020 : 463) على ضرورة تطبيق الأمن السيبراني ونشر ثقافته وتوعية الأفراد والمؤسسات به، وجاء للأهداف التالية:

1. تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.
2. التصدي لهجمات وحوادث امن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.
3. توفير بيئة أمنة موثوقة للتعاملات في مجتمع المعلومات، وتوفير بنى تحتية لديها حساسية للهجمات الإلكترونية.
4. توفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.
5. التخلص من نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها.
6. سد الثغرات في أنظمة أمن المعلومات.
7. مقاومة البرمجيات الخبيثة، لما تستهدفه من إحداث أضرار بالغة للمستخدمين.
8. الحد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.
9. اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة.

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

10.تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية بقصد الضرر بمعلوماتهم الشخصية سواء بالإتلاف أو بقصد السرقة.

2-3 أهمية الأمن السيبراني

إن ارتباط الأمن السيبراني بالتحول الرقمي الناجح يعتمد على أُطر وآليات حكومية وبيئة تشريعية متقدمة داعمة للرقمنة والبنية التحتية المتقدمة، فالجرائم الإلكترونية تتم بمنهجية وأساليب متطورة، لذلك كان الأمن السيبراني الحل للتغلب على هذه الجرائم بما يتميز به من خصائص نذكر منها الآتي:

1. الإكتشاف والتعقب: يهدف اكتشاف الجرائم الإلكترونية وتعقب أثرها إلى التغلب عليها .
2. السرعة وغياب الدليل: إن استخدام وسائل تقنية حديثة من قبل المخترقين جعل من الصعب إثبات هذه الجرائم لذلك أتى الأمن السيبراني بتقنيات عالية الحداثة تفوق خبرة المخترقين (عبد الفتاح بيومي، 198،2007).
3. الأمن السيبراني كان الحل لتعزيز الأمن الرقمي للهيئات الحكومية والمؤسسات التعليمية نتيجة لضعف الأجهزة الأمنية في التعامل مع الجرائم الإلكترونية لما تفتقره من خبرة في هذا المجال (فؤاد الملاحي، 129 ،2015)
4. السرية (Confidentiality) : أي التحكم في الولوج إلى البيانات وإتاحتها لمن يُسمح لهم فقط.
5. السلامة (Integrity): الحفاظ على سلامة البيانات والمعلومات وحمايتها من الهجمات التخريبية أو السرقة.
6. الجاهزية (Availability): جاهزية جميع الأنظمة والخدمات والمعلومات وإتاحتها حسب طلب الشركة أو عملائها.

2-4 التهديدات الالكترونية والهجمات السيبرانية وطرق الوقاية منها:

الجدول رقم(1) يوضح التهديدات الالكترونية المختلفة وكيفية الوقاية منها

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

جدول .1. التهديدات الالكترونية وطرق الوقاية

التهديدات الإلكترونية	طرق الوقاية
البرامج الضارة Malicious Codes يتسّم هذا الخطر بأنّه من أشهر أنواع المخاطر التي تُهدد الأمن السيبراني خاصةً والإنترنت عامةً، إذ تتسلل بعض البرامج إلى الأنظمة، وتُثبّت نفسها على النظام بهدف الوصول غير المصرح به للبرامج والملفات، وإلحاق الضرر بها، وربما حذفها أو سرقتها.	ويُمكن الوقاية من خطر البرامج الضارة من خلال تثبيت البرامج الخاصة بمكافحة البرامج الضارة والتعرف عليها، مع ضرورة التحديث المستمر لهذه البرامج، والمراقبة الدائمة لوجود أيّ ملفات أو روابط غير معروفة.
سرقة كلمة المرور Passwords penetration يُمكن ملاحظة هذا الخطر بمجرد محاولة الدخول إلى الحساب، إذ يتبين وجود تغيير في كلمة المرور، وهذا مؤشر على أنّ شخص ما تمكّن من اختراق النظام والحصول على كلمة المرور، وهذا حتمًا يُشير إلى الخطر الذي يُحيط بالبيانات السرية الموجودة على النظام.	ويُمكن الوقاية من هذا الخطر من خلال تطبيق نظام المصادقة الثنائية، والتي تتطلب خطوات إضافية من أجل تسجيل الدخول، وتُعَد هذه الخطوات من الطرق التي تُساعد على تعقيد عمليات تسجيل الدخول للأنظمة.
التنصت Eavesdrop on data يتمثل هذا الخطر في قدرة أحد الأطراف على الاستماع للبيانات المتنقلة بين المستخدم والمضيف، وهذا يعني سرقة المعلومات من النظام، وعادةً ما تختلف المعلومات المسروقة بناءً على حركة التنصّت المطبّقة	وللوقاية منها يتم تثبيت برامج (VPN)، أو تجنّب الدخول لمواقع الانترنت المخترقة.
هجمات التصيد Data phishing attacks يكون التصيد على شكل رسائل من جهات رسمية تتضمن طلب كلمات المرور، أو بعض البيانات الهامة، وهُنا يقع بعض الأشخاص في الخطأ، ويُقدّم معلومات هامة للمتصيدين من خلال النقر على رابط مشبوه مثلًا.	يُمكن الوقاية من هذه الطريقة من خلال الحرص على البيانات الخاصة، وعدم الإدلاء بها لأي شخصٍ كان، إلّا بعد التيقّن من الجهة المقابلة، ويجدر بالأشخاص الانتباه إلى أنّ رسائل التصيّد عادة ما تكون مليئة بالأخطاء الإملائية والنحوية، وممّا يجدر ذِكره بأنّ الرسائل المستقبلة من الجهات الرسمية عادةً لا تتضمّن طلب بيانات خاصة.

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

رفض الخدمة الموزع DDoS – Data Distributed Denial of Service يستهدف هذا الخطر عادةً الخوادم الرئيسية، وفي هذه الحالات يُوقف الخادم مواقع الويب التي تُحاول الوصول للبيانات، أو يحدث بطء في أداء الخوادم	ويُمكن الوقاية من هذا الخطر من خلال إيقاف الوصول عن طريق قطع الإنترنت عن الخوادم
هجوم عبر الموقع Cross-site attack on data يُنفّذ هذا الخطر من خلال استهداف مواقع الويب الضعيفة، وتحميل عدد من الرموز الخطيرة عليها، وفي حال دخول أحد المستخدمين لهذه المواقع سرعان ما يتعرّض النظام الخاص به للسرقة، أو التسبب بتعطل الخدمات الرئيسية فيه	ويُمكن الوقاية من خطر هذا الهجوم من خلال تطبيق أمر إيقاف تشغيل البرامج النصية للصفحات، أو تثبيت الوظائف الخاصة بحظر البرامج النصية على المتصفح.
هجومSQL : يُعدّ هذا الهجوم برنامج لمعالجة البيانات، بحيث يُتاح للأطراف الخارجية الوصول للمعلومات غير المتاحة، والمعلومات الحساسة من خلال عدد من البرمجيات.	ويُمكن الوقاية من هذا الخطر من خلال تطبيق جدران الحماية الذكية، أو التحديث الدائم للتعليمات البرمجية التي تستطيع التعرّف على التداخلات غير القانونية.
برامج الفدية Ransomware تُثبت عدد من البرامج الضارة على الأنظمة، ممّا يؤدي إلى منع الوصول إلى النظام، وبالتالي يطلب الطرف الخارجي من المستخدم دفع الفدية مقابل إزالة هذه البرامج	ويُمكن للمستخدم الوقاية من هذه البرامج من خلال التحديث الدائم لبرامج مكافحة الفيروسات، والحرص على عدم فتح الروابط الضارة.
فيروس طروادة Trojan Horse يُمكن دخول للنظام من خلال تنكّره ببرامج قانونية من خلال التنبيهات التي تُظهر للمستخدم حاجة النظام الخاص به للمسح الضوئي، وهُنا تستطيع البرامج الضارة الدخول للنظام من خلال عملية المسح.	ويُمكن الوقاية من هذا الخطر من خلال الحرص على عدم تنزيل أي برامج غير معروفة المصدر.

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

ثالثا الجانب العملي للدراسة:

3-1 منهج الدراسة

منهج الدراسة هو الطريق أو المسلك الذي يسير فيه الباحث للوصول إلى المعرفة، وذلك عن طريق إتباع مجموعة من القواعد والعمليات التي يتبعها العقل والحس للوصول إلى غاية أو نتيجة محددة. وفى ضوء طبيعة هذه الدراسة والأهداف التي تسعى إلى تحقيقها ومن خلال التساؤلات التي تسعى هذه الدراسة للإجابة عليها فقد استخدم الباحث المنهج الوصفي التحليلي، الذي يقوم على دراسة الواقع أو الظاهرة كما هي في الواقع ، ويهتم بوصفها وصفاً دقيقاً، حيث يتلاءم الأسلوب الوصفي مع الهدف النظري لهذه الدراسة والمتمثل في التعرف على المفاهيم الخاصة بهذه الدراسة، في حين يتلائم الأسلوب التحليلي مع الهدف العملي لها، ولا يتوقف هذا المنهج على جمع المعلومات والبيانات المتعلقة بالظواهر أو الواقع كما هو بل يتعداه إلى الوصول إلى استنتاجات تسهم في فهم الواقع وتطويره.

3-2 مجتمع الدراسة

يشمل مجتمع هذه الدراسة الأصلي جميع هيئة التدريس بالجامعات الليبية وتمثله عينة الدراسة في هيئة التدريس بجامعة الزاوية والبالغ عددهم (138) وقد تم الاعتماد على اسلوب المسح الشامل لصغر حجم مجتمع الدراسة.

3-3 أداة الدراسة:

لتحقيق أغراض البحث وبعد الاطلاع على الدراسات السابقة التي تتعلق بموضوع هذا البحث، قام الباحثون بتصميم أداة البحث والذي كان بعنوان: "مدى وعي أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبراني في ظل التحول الرقمي.

اشتملت الأداة على ثلاثة أقسام: تضمن القسم الأول معلومات عن المستقصى منهم شملت متغيرات الجنس، المؤهل العلمي، الخبرة العملية، وتضمن القسم الثاني وهو المتعلق بدرجة الأمن السيبراني (24 فقرة)، وتضمن القسم الثالث انتهاكات و مخاطر الأمن السيبراني, ويتضمن (6فقرات).

حيث وزعت استمارة الاستبيان بشكل الكتروني وكان عدد الاستمارات التي خضعت للتحليل الإحصائي (78) استمارة.

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

3-4 الصدق أداء الظاهري:

للتأكد من صدق مقياس الدراسة قام الباحثون بعرض استمارة الاستبانة على مجموعة من المحكمين من ذوي الخبرة والاختصاص في الجامعات الليبية. وذلك لإبداء رأيهم وتقديم مقترحاتهم حول استمارة الاستبانة، والاستفادة من خبراتهم في الحكم على المقاييس المستخدمة ومدى ملاءمتها للتطبيق في الدراسة، وبناء على الملاحظات القيمة الواردة من المحكمين تم إجراء التعديلات على استمارة الاستبانة بشكلها النهائي.

1. صدق المقياس (الاتساق الداخلي):

يقصد بصدق المقياس (الاتساق الداخلي) مدى اتساق كل فقرة من فقرات الاستبانة مع المجال الذي تنتمي

إليه هذه الفقرة وقد تم حساب الاتساق الداخلي للاستبانة وذلك من خلال حساب معاملات الارتباط (معامل

ارتباط سيبرمان) بين كل فقرة من فقرات مجالات الاستبانة والدرجة الكلية للمجال نفسه.

- المتغير الأول: درجة الأمن السيبراني.

يوضح الجدول (2) معامل الارتباط بين كل فقرة من فقرات المجال الأول والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة بالجدول دالة إحصائية عند مستوى دلالة (0.000) أقل من مستوى معنوية 0.05 وبذلك يعتبر المجال صادق لما وضع لقياسه.

جدول .2. معامل الارتباط بين كل فقرة من فقرات المجال الأول والدرجة الكلية

ت	العبـــــارة	معامل الارتباط	مستوى الدلالة
	متغير درجة الأمن السيبراني		
1	أختار كلمه مرور قوية تحتوي على مجموعة من الأحرف والأرقام والرموز.	. 712	0.000
2	أتجنب فتح أي رابط من شخص غير معروف	.704	0.000
3	أحرص على عدم فتح أي رسائل الكترونية مجهولة المصدر	.763	0.000
4	أتجنب إرسال معلوماتي الشخصية عبر الرسائل النصية أو البريد الالكتروني	.711	0.000
5	احرص على استخدام متصفح آمن للإنترنت	.571	0.000

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

6	أحذر كثيراً عند الاتصال بالشبكات العامة	.590	0.000
7	أتوخى الحذر عند مشاركة الآخرين معلومات حساسة باستخدام إعدادات الخصوصية للخدمات الالكترونية	.782	0.000
8	احرص على تحميل التحديثات والبرامج الآمنة	.621	0.002
9	الغي أي اشتراك لي في الإعلانات المستهدفة لحماية بياناتي الشخصية والمالية	.812	0.000
10	استخدم أدوات الإبلاغ عن الإساءات التى يتعرض لها المستخدمون	.562	0.001
11	استخدم تقنية التحقق الثنائى (كلمه المرور – البصمة)	.631	0.001
12	احرص على تحميل برامج حماية ضد المواقع الضارة	.577	0.000
13	اهتم بتحميل برامج آمنة لمكافحة الفيروسات	.809	0.000
14	افحص الروابط التي تبدو لي أنها ضارة	.489	0.000
15	ادعم البيانات المخزنة على جهازي بإعداد نسخة احتياطية في ذاكرة خارجية أو على الخدمة السحابية	.621	0.003
16	احرص على تعطيل خدمات الوصول لموقعي فى التطبيقات المحملة على جهازي	.477	0.001
17	احرص على غلق جهازي الحاسوب بشكل صحيح تحسبا لفقد أي بيانات أو معلومات	.701	0.000
18	أغير إعدادات جهازي بشكل مستمر حفاظا على اختراق شبكة الواي فاي.	.722	0.001
19	أتجنب الكشف عن أي بيانات شخصية أو عائلية أثناء تصفحي على الإنترنت	.833	0.000
20	احرص على الإبلاغ عن المواقع المشكوك فيها للجهات المختصة	.790	0.000
21	أفضل استخدام التشفير عند إرسال معلومات هامة عبر الانترنت	.671	0.000
22	أؤيد عمل دورات تدريبية في مجال الأمن السيبراني	.781	0.001
23	اراعي النزاهة في هويتي الرقمية حين استخدم مواقع التواصل الالكتروني	.609	0.000
24	إنا مع وضع إجراءات وسياسات لحفظ الأمن السيبراني في كافة الجامعات	.521	0.000

- **المتغير الثاني : انتهاكات و مخاطر الأمن السيبراني.**

يوضح الجدول (3) معامل الارتباط بين كل فقرة من فقرات المجال الأول والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة بالجدول دالة إحصائية عند

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

مستوى دلالة (0.000) أقل من مستوى معنوية0.05 وبذلك يعتبر المجال صادق لما وضع لقياسه.

جدول.3. معامل الارتباط بين كل فقرة من فقرات المجال الأول والدرجة الكلية

ت	العبـــــــارة	معامل الارتباط	مستوى الدلالة
	متغير انتهاكات و مخاطر الأمن السيبراني.		
1	أتجنب المعلومات التي من شانها المساس بالأمن القومي	597.	0.000
2	احترم اللوائح و القوانين المتبعة في الدولة عند التعامل مع شبكة الانترنت	.690	0.001
3	استخدم المحتوى المرخص من قبل الناشر أو المؤلف	.599	0.000
4	احترم سياسة المواقع الالكترونية التي استخدامها	826.	0.000
5	احرص على عدم تبادل أرقام الحسابات والبطاقات المصرفية عبر الانترنت	.781	0.002
6	أتجنب تعبئة البيانات الشخصية و الأرقام الوطنية في أي نموذج غير موثوق المصدر على الانترنت	521.	0.000
7	اقترح أن تقوم الجامعة بعمل ندوات وورش عمل ودورات في مجال الأمن السيبراني	.632	0.000

- **ثبات أداة الدراسة:**

يقصد بثبات أداة الدراسة والمتمثلة في الاستبانة ان تعطي هذه الاستبانة النتيجة ذاتها لو تم إعادة توزيعها أكثر من مرة تحت نفس الظروف والشروط، وقد اتضح أن معامل **ألفا كرونباخ** جيد حيث بلغ معامل الثبات الكلي للاستبيان(0.893) كما هو موضح في الجدول التالي:

الجدول.4. معامل ثبات الدراسة

ت	متغيرات الدراسة	الفقرات	معامل الثبات
1	درجة لأمن السيبراني	24	0.805
2	انتهاكات و مخاطر الأمن السيبراني	7	0.741
	الثبات الكلـــــى	31	0.893

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

- **خصائص عينة الدراسة: تتمثل خصائص الأفراد عينة الدراسة بالفقرات الموضحة بالجدول رقم(5) التالي:**

الجدول .5. توزيع عينة الدراسة حسب الخصائص الشخصية والوظيفية

المتغير	فئات المتغير	العدد	النسبة %
الجنس	ذكر	40	51
	أنثى	38	49
	المجمـــوع	78	100
المؤهل العلمي	ماجستير	48	62
	دكتوراه	30	38
	المجمـــوع	78	100
سنوات الخبرة	من 1 - 3 سنوات	5	5
	من 3 - 10 سنوات	28	36
	من 10 – 15 سنة	25	32
	أكثرمن 15 سنة	20	27
	المجمـــوع	78	100
الإجمـــــالي		78	100

- **المصدر: إعداد الباحثين بالاعتماد على نتائج برنامج SPSS**

- **التوزيع حسب المؤهل العلمي:** بالنظر في الجدول السابق يتضح أن عدد الذين يحملون مؤهلات علمية ماجستير (48) مفردة بنسبة (62%)، وعدد الذين يحملون مؤهلات علمية دكتوراه (30) مفردة بنسبة (38%)،من جملة عينة الدراسة التي تبلغ (78) مفردة بنسبة (100%)، وهذا مؤشر جيد على أن أفراد عينة الدراسة على قدر جيد من التأهيل العلمي يؤهلهم للإجابة على أسئلة الاستبيان .

- **التوزيع حسب سنوات الخبرة :** بالنظر في الجدول السابق يتضح أن عدد الأفراد الذين خبرتهم من سنة إلي 3 سنوات (5) فرداً بنسبة (5%)، وعدد الأفراد الذين خبرتهم من 3 إلى 10 سنوات (28) فرداً بنسبة (36%)، وعدد الأفراد الذين خبرتهم من 10 – 15 سنة (25) فرداً بنسبة (32%)، وعدد الأفراد الذين خبرتهم من 15 سنة فأكثر (20) فرداً بنسبة (27%) من جملة عينة الدراسة التي تبلغ (78) فرداً بنسبة (100%)، وهذا يدل على وجود خبرات متفاوتة بين أفراد عينة الدراسة.

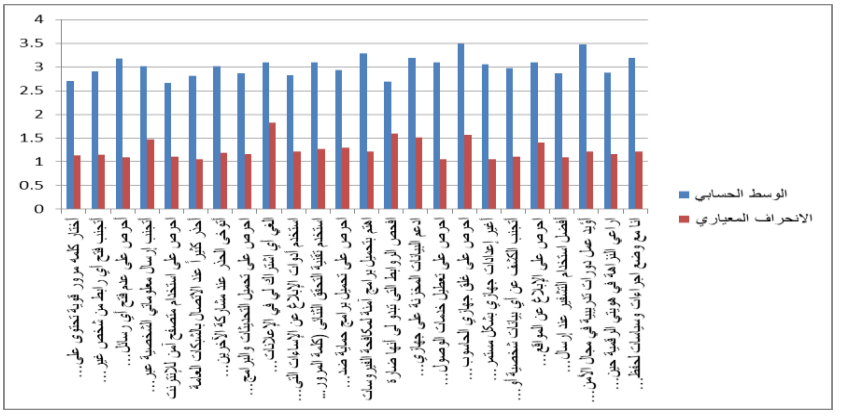
Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

3- 5 وصف متغيرات الدراسة

توصف متغيرات الدراسة في هذا الجزء بمقاييس النزعة المركزية، ممثلة بالوسط الحسابي، ومقاييس التشتت المطلق، ممثلة بالانحراف المعياري، كما يأتي:

- **المتغير الأول:(درجة الأمن السيبراني)**

تم قياس المتغير **درجة الأمن السيبراني** بأربعة وعشرين فقرة والشكل رقم(1) يبين فقرات قياس هذا المتغير والوسط الحسابي والانحراف المعياري ومستوى اتجاه أفراد العينة.



الشكل .1. الوسط الحسابي والانحراف المعياري لفقرات متغير درجة الأمن السيبراني:

المصدر: إعداد الباحثين بالاعتماد على نتائج برنامج SPSS

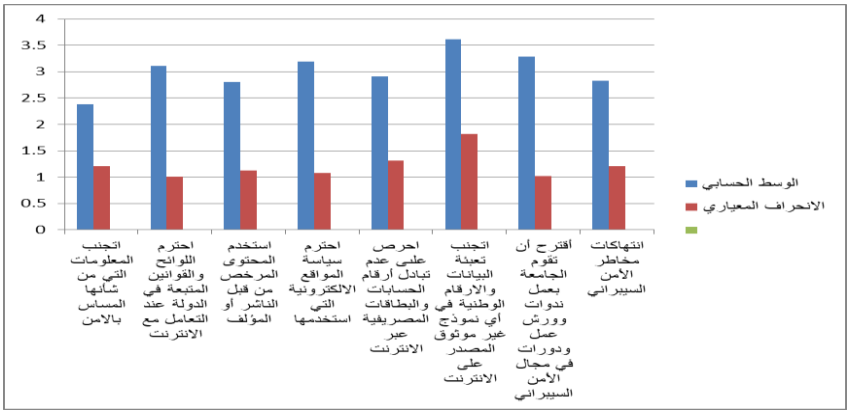
يتضح من الشكل رقم (3-4) أن الفقرة التي تنص على أن: (احرص على غلق جهازي الحاسوب بشكل صحيح تحسبا لفقد أي بيانات أو معلومات) حصلت على المرتبة الأولى بمتوسط حسابي **(3.49)** وانحراف معياري **(1.57)**، مما يدل على أن أعضاء هيئة التدريس يحرصون على غلق جهاز الحاسوب بشكل صحيح تحسبا لفقد أي بيانات أو معلومات وهذا يدل على أنهم على داريه بعمليات الاختراق، في حين حصلت الفقرة التي تنص على ما يأتي: (احرص على استخدام متصفح آمن للإنترنت) حصلت على المرتبة الأخيرة، من بين جميع فقرات هذا المتغير، بمتوسط حسابي (2.66) وانحراف معياري

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

(1.11)، وبمقارنة المتوسطات الحسابية لجميع فقرات متغير درجة الأمن السيبراني بالوسط النظري المعتمد في الدراسة نلاحظ أن اتجاهات أفراد عينة الدراسة حول المتغير كانت ايجابية، وأخيراً بلغ المتوسط الحسابي الكلي لمتغير درجة الأمن السيبراني (3.21) وبانحراف معياري (1.04)، مما يؤكد أن اتجاهات أفراد العينة حول متغير درجة الأمن السيبراني كانت ايجابية.

- **المتغير الثاني (انتهاكات ومخاطر الأمن السيبراني):**

تم قياس المتغير انتهاكات ومخاطر الأمن السيبراني بسبع فقرات والشكل رقم(2) يبين فقرات قياس هذا المتغير والوسط الحسابي والانحراف المعياري ومستوى اتجاه أفراد العينة.



الشكل .2. الوسط الحسابي والانحراف المعياري لفقرات متغير: انتهاكات ومخاطر الأمن السيبراني

المصدر: إعداد الباحثين بالاعتماد على نتائج برنامج SPSS

يتضح من الشكل رقم (3-5) أن الفقرة التي تنص على أن: (أتجنب تعبئة البيانات الشخصية و الأرقام الوطنية في أي نموذج غير موثوق المصدر على الانترنت) حصلت على المرتبة الأولى بمتوسط حسابي **(3.61)** وانحراف معياري **(1.82)**، مما يدل على أن عينة الدراسة يتجنبون تعبئة البيانات الشخصية و الأرقام الوطنية في أي نموذج غير

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

موثوق المصدر على الانترنت، في حين حصلت الفقرة التي تنص على ما يأتي: (استخدم المحتوى المرخص من قبل الناشر أو المؤلف) حصلت على المرتبة الأخيرة، من بين جميع فقرات هذا المتغير، بمتوسط حسابي (2.81) وانحراف معياري (1.13)، مما يدل على أن عينة الدراسة يستخدمون المحتوى المرخص من قبل الناشر أو المؤلف، وبمقارنة المتوسطات الحسابية لجميع فقرات المتغير التي تتعلق بانتهاكات و مخاطر الأمن السيبراني بالوسط النظري المعتمد في الدراسة نلاحظ أن اتجاهات أفراد عينة الدراسة حول المتغير كانت ايجابية ، وأخيراً بلغ المتوسط الحسابي الكلي لمتغير انتهاكات و مخاطر الأمن السيبراني **(2.83)** وبانحراف معياري **(1.21)**، مما يؤكد أن اتجاهات أفراد العينة حول متغير انتهاكات و مخاطر الأمن السيبراني كانت ايجابية.

3-6 اختبار فرضيات الدراسة:

-الفرضية الصفرية:

-يوجد وعي من قبل أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبراني في ظل التحول الرقمي.

-الفرضية العدمية:

-لا يوجد وعي من قبل أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبراني في ظل التحول الرقمي.

ولاختبار الفرضية فقد تم استخدام اختبار الانحدار واختبار F الناتج عنه, لمعرفة أن كان هناك فروق ذات دلالة بين متوسطات تقديرات أفراد عينة الدراسة للعلاقة بين **وعي أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبراني في ظل التحول الرقمي** في محل الدراسة, على مستوى الدلالة الإحصائية (α =0.05) ويبين الجدول رقم (6) النتائج المتعلقة بتحليل هذه العلاقة.

الجدول رقم.6. نتائج اختبار الانحدار و اختبار F الناتج عنه

R الارتباط	الارتباط المصحح R^2	F	مستوى الدلالة	نتيجة الفرضية
0.759	0.576	128.622	0.000	قبول

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

لقد جاءت قيمة اختبار (F) مساوياً إلى (128.622) بقيمة احتمالية (0.000) وهي أقل من القيمة المحددة (0.05) مما يشير إلى وجود علاقة ذات دلالة إحصائية بين **وعي أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبراني في ظل التحول الرقمي** في محل الدراسة، بالتالي نقبل الفرضية الصفرية التي تنص على انه يوجد وعي من قبل أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبراني في ظل التحول الرقمي، ونرفض فرضية العدم ويتضح من الجدول نفسه أن المتغير المستقل (وعي أعضاء التدريس) في هذا النموذج يفسر ما مقداره (57%) من التباين في المتغير التابع (الأمن) وهي قوة تفسيرية جيدة ، مما يدل على أن هناك أثراً للمتغير المستقل في المتغير التابع.

رابعا: النتائج والتوصيات.

- **النتائج:**
- يوجد وعي بنسبة كبيرة من قبل أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبراني في ظل التحول الرقمي.
- **التوصيات:**

1. الإيمان بأن الأمن السيبراني أفضل وأقصر الطرق لحماية البيانات والأنظمة.
2. عقد دورات تدريبية لأعضاء هيئة التدريس تخص الأمن السيبراني.
3. إقامة ورش عمل بشكل دوري لاطلاع أعضاء هيئة التدريس على أخر التطورات في مجال الأمن السيبراني وإجراءات الحماية من المخاطر والانتهاكات السيبرانية.
4. توصية وزارة التعليم العالي والعام إدراج مجال الأمن السيبراني ضمن مناهج التعليم في المدارس والجامعات لتوعية الطلاب.
5. تشجيع بحوث ودراسات الأمن السيبراني وإجراء دراسات حول مخاطر الجرائم السيبرانية.

- **المراجع والمصادر:**

الاتحاد الدولي للاتصالات. (2011). الاتجاهات في مجال الاتصالات: تمكين تاريخ الاسترجاع: 14/مايو/ 2021

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

الجندي، علياء بنت عبد الله ومحمد، نهير طه. (2019). دور الممارسة التطبيقية للأمن السيبراني في تنمية المهارات ودقة التطبيق العملي للأمن المعلومات لدى طالبات الجامعة ، مجلة عالم التربية – المؤسسة العربية للاستثمارات العلمية وتنمية الموارد البشرية ع (67)، ج (3)، ص14-84.

السمحان، منى عبد الله (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. مجلة كلية التربية – جامعة المنصورة ع (111)، ح (1)، ص2–29.

الصانع، نورة عمر وسليمان، إيناس السيد محمد وعسارن، عواطف سعد الدين والسواط، حمد بن حمود وأبو عميشة، زاهدة جميل (2020) وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم. مجلة كلية التربية جامعة أسيوط .م(36) – ، ع (6) ، ص 41 –90.

الصلاحي، فؤاد (2015). الأمن السيبراني، مجلة الدوحة، وزارة الأعلام، قطر .

العريشي، جبريل حسن والدوسري، سلمى بنت عبد الرحمن. (2018) دور مؤسسات التعليم العالي في تعزيز ثقافة امن المعلومات في المجتمع. مجلة مكتبة الملك فهد الوطنية – مكتبة فهد الوطنية. م (24)، ع (2)، ص 302–373.

الغامدي، سارة أحمد. (أكتوبر/ 2018). مبادرة العطاء الرقمي، تم الاسترجاع من الرابط https://attaa.sa/arabic-content/view/20: بتاريخ17/مايو/2021م.

القحطاني، نورة بنت ناصر . (2019). مدى توافر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دراسة ميدانية. مجلة شؤون اجتماعية–جمعية الاجتماعيين في الشارقة. م (36)، ع (144)، ص 85–120.

الموجي، كوثر السعيد ومحمود دينا كمال وإمام، أحمد عزمي. (2021). تصور مقترح لتفعيل الأمن السيبراني بوزارة ومديريات الشباب والرياضة بجمهورية مصر العربية. مجلة بني سويف لعلوم التربية البدنية والرياضية. م(4)، ص(7)، ص14–38.

المشر ، عبداطمة يوسف وحريري، رندة (2020). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. المجلة العربية للتربية النوعية. م (4)، ع (13)، ص 95–140.

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

بيومي،عبد الفتاح (2007). مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر.

- **المراجع الأجنبية:**

Wijayanto, H., & Prabowo, I. A. (2020).. Cyber security Vulnerability Behavior Scale in College during the Covid-19 Pandemic. Jurnal Sisfokom (Sistem Information dan Komputer), 9(3), 395-399.

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية